Risiko Supply Chain: Sichere Systeme dank Sealed Platform?

23.07.2019 – München: 183 Millionen Pfund Strafe – damit haben die Verantwortlichen bei British Airways (BA) nicht gerechnet! Verstöße gegen Datenschutzauflagen können teuer werden, seit die DSGVO Anwendung findet; das erfährt die britische Fluglinie nun am eigenen Portemonnaie[1]. Dabei ist der Reputationsverlust noch gar nicht beziffert! Wir erinnern uns: Bei einem Hackerangriff 2018 hatten Angreifer Daten von rund 500.000 Kunden gestohlen. Nun, knapp ein Jahr später, wird BA zur Kasse gebeten – und das nicht zu knapp.

Hohe Strafen drohen auch den Unternehmen, die Dienste des indischen Tech-Dienstleisters Wipro in Anspruch nehmen und damit ihre Datenschutzpflichten verletzen[2]. Der IT-Zulieferer ist seit 2017 verstärkt das Ziel von Cyberkriminellen, die es vornehmlich auf Wipros Kunden abgesehen haben. Darunter: Internet-Anbieter, Versicherungsgesellschaften und Energieprovider.

Was beide Fälle gemeinsam haben? Schwachstellen in der Supply Chain – ein Risiko, das viele Zulieferer und Unternehmen unterschätzen. Doch wie kann man diese vermeiden?

Gefahren des Supply Chain Management

Ziel des Supply Chain Management ist vor allem, sämtliche Prozesse entlang der gesamten Liefer- und Wertschöpfungskette zu optimieren. Dazu stehen den Partnern im Idealfall geeignete Schnittstellen zur Verfügung; außerdem herrscht ein hohes Maß an Vertrauen zwischen den beteiligten Unternehmen, sodass sich Zulieferer und Abnehmer beispielsweise über Probleme der eigenen Lieferketten informieren können.

Trotzdem kommt es immer wieder zu Störungen. Neben solchen, die in der Wertschöpfungskette selbst auftreten können – etwa kurzfristige Lieferengpässe oder Produktionsausfälle[3] – sind das vor allem Datenschutzvorfälle.

Das liegt daran, dass Zulieferer auf Daten eines Unternehmens zugreifen können müssen und mit den Mitarbeitern häufig noch weitere Informationen austauschen. Damit erweitern sie die Angriffsfläche für Hacker und Cyberkriminelle. Eine andere Gefahr besteht darin, dass interne Angreifer – etwa Mitarbeiter oder Administratoren – sich unerlaubt Zugang zu vertraulichen Informationen verschaffen und diese entwenden, beschädigen oder manipulieren.

Wie geht sicheres Supply Chain Management?

Um Risiken zu minimieren und kostspielige Datenschutzverstöße von vornherein möglichst auszuschließen, sollten Unternehmen ihre Supply Chain absichern – so wie grundsätzlich alle datenverarbeitenden Systeme angemessen zu schützen sind. Das betrifft nicht nur die Softwareseite, sondern ganz besonders die zugrundeliegende Infrastruktur.

Dabei spielt es keine Rolle, ob Unternehmen und Zulieferer auf Cloud-Angebote von Drittanbietern zurückgreifen oder eigene Server-Infrastrukturen nutzen – die Sicherheitslücken sind in der Regel dieselben. Denn oft setzen Betreiber auf eine Kombination aus „technischen und organisatorischen Maßnahmen[4]“, um Daten gegen Angriffe und Verluste zu schützen. Hier besteht jedoch stets das Risiko, dass die organisatorischen

[1] https://www.bbc.com/news/business-48905907
[2] https://www.forbes.com/sites/kateoflahertyuk/2019/04/16/breaking-down-the-wipro-breach-and-what-it-means-for-supply-chain-security/#442914205259
[3] https://www.riskmethods.net/media/Content/Whitepapers/bme-lieferkette-so-mindern-sie-risiken.pdf
[4] https://dsgvo-gesetz.de/art-32-dsgvo/

Maßnahmen umgangen werden und sich Mitarbeiter des Betreibers oder Administratoren unerlaubt Zugang zu sensiblen Daten verschaffen

Sealed Platform: Sicherheit durch Versiegelung?

Geht das auch sicherer? Ja: Mehr Schutz als gängige Clouds und Serveranlagen bieten versiegelte Infrastrukturen wie Uniscons Sealed Platform. Statt technische und organisatorische Maßnahmen zu kombinieren, setzt die Münchner TÜV SÜD-Tochter auf einen Satz rein technischer Schutzmaßnahmen. Die lassen sich auch mit großem Aufwand nahezu nicht umgehen – nicht einmal durch den Serverbetreiber oder Administratoren.

Dafür sorgen unter anderem mit Sensoren abgesicherte Käfige, ein gehärtetes Betriebssystem und Schnittstellen mit speziellen Filtern. Ein aufwändiger Versiegelungsprozess durch unabhängige Prüfstellen stellt schließlich die Integrität der Server und somit die Unversehrtheit der darauf gespeicherten und verarbeiteten Daten sicher.

Uniscons hochsichere Cloud-Plattform sorgt dafür, dass eine sichere Software nicht durch Lücken in der Infrastruktur kompromittiert wird. So lassen sich Anwendungen zum Supply Chain Management soweit absichern, dass unerwünschte Datenzugriffe praktisch unmöglich sind – und teure Strafzahlungen wie im Fall British Airways vermieden werden.

Weiterführende Informationen zur Sealed Platform sowie druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de.

Uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die Uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet Uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist Uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zu Partnern und Produkt: www.uniscon.com

Pressekontakt

Uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20